

Beleid

Informatiebeveiliging & privacy

Inleiding

Vanaf 25 mei 2028 geldt de Algemene verordening gegevensbescherming (AVG) voor alle lidstaten van de EU. Stichting WijWijzer scholen (WijWijzer) is vanaf begin 2018 conform deze verordening gaan werken en heeft de organisatie hierop ingericht. Op basis van voortschrijdend inzicht binnen onze stichting, maar ook in onze omgeving en bij samenwerkingspartners heeft dit zijn beslag gelegd op hoe wij met elkaar en de buitenwereld communiceren en hoe wij onze administratieve en ICT-organisatie hebben vormgegeven.

In dit document lezen medewerkers en externen (ouders, toezichthouders) op welke manier de AVG in onze organisatie verankerd is.

Het beleid Informatiebeveiliging & privacy is onder verantwoordelijkheid van het College van Bestuur tot stand gekomen, met instemming van de GMR.

Veel gebruikte afkortingen

- AVG Algemene verordening gegevensbescherming
- IBP Informatiebeveiliging en privacy
- AP Autoriteit persoonsgegevens
- FG Functionaris voor gegevensbescherming
- PO Privacy officer
- SO Security officer

Inhoudsopgave

Inleiding.....	1
Inhoudsopgave.....	2
1. Het belang van informatiebeveiliging en privacy.....	3
2. Toelichting informatiebeveiliging en privacy.....	3
2.1. Wat verstaan we onder informatiebeveiliging?.....	3
2.2. Wat verstaan we onder privacy.....	3
2.3. Vervlechting informatiebeveiliging en privacy.....	3
3. Doel en reikwijdte.....	4
3.1. Doel.....	4
3.2. Reikwijdte.....	4
4. Beleid: hoe doen we dat?.....	5
5. Uitwerking van het beleid: wat doen we?.....	6
5.1. Relevante wet- en regelgeving.....	6
5.2. Basisregels bij het omgaan met persoonsgegevens.....	7
5.3. Ondersteunende richtlijnen en procedures.....	7
5.8. Naleving en sancties.....	8
5.9. Logging en monitoring.....	9
6. Organisatie: wie doet wat?.....	9
6.1. Rollen en verantwoordelijkheden.....	9
6.2. Richtinggevend.....	9
6.4. Uitvoerend.....	10
BIJLAGE 1: Ondersteunende regelingen en procedures.....	12
BIJLAGE 2: Overzicht van rollen en verantwoordelijkheden en taken.....	13

1. Het belang van informatiebeveiliging en privacy

Het onderwijs is in toenemende mate afhankelijk van informatie en ict. De hoeveelheid informatie, waaronder persoonsgegevens, neemt toe door o.a. ontwikkelingen als gepersonaliseerd leren met behulp van ict. Het is belangrijk om informatie goed te beschermen en veilig en verantwoord met persoonsgegevens om te gaan. De afhankelijkheid van ict en persoonsgegevens brengt nieuwe kwetsbaarheden en risico's met zich mee. Het goed regelen van informatiebeveiliging en privacy (IBP) in een IBP-beleid is noodzakelijk om de gevolgen van deze risico's tot een aanvaardbaar niveau te reduceren en de voortgang van het onderwijs en de bedrijfsvoering optimaal te kunnen waarborgen.

2. Toelichting informatiebeveiliging en privacy

2.1. Wat verstaan we onder informatiebeveiliging?

Onder informatiebeveiliging wordt verstaan het nemen en onderhouden van een hoeveelheid samenhangende maatregelen zodat de betrouwbaarheid van de informatievoorziening gegarandeerd kan worden.

Informatiebeveiliging richt zich op de volgende aspecten:

- *Beschikbaarheid (B)*: de mate waarin gegevens en/of functionaliteiten beschikbaar zijn op de juiste momenten.
- *Integriteit (I)*: de mate waarin gegevens en/of functionaliteiten juist en volledig zijn.
- *Vertrouwelijkheid (V)*: de mate waarin de toegang tot gegevens en/of functionaliteiten beperkt is tot degenen die daartoe bevoegd zijn.

Onvoldoende informatiebeveiliging kan leiden tot ongewenste risico's in het onderwijsproces en bij de bedrijfsvoering van de instelling. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades en imagooverlies.

2.2. Wat verstaan we onder privacy

Privacy gaat over persoonsgegevens. Persoonsgegevens moeten beschermd worden volgens de huidige wet- en regelgeving. Bescherming van de privacy regelt onder andere onder welke voorwaarden persoonsgegevens verwerkt mogen worden. Persoonsgegevens zijn hierbij alle gegevens die een natuurlijke persoon direct of indirect kunnen identificeren. Onder verwerking wordt elke handeling met betrekking tot persoonsgegevens verstaan.

De wet noemt als voorbeelden van verwerking:

Het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekking door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens.

2.3. Vervlechting informatiebeveiliging en privacy

Uit voorgaande blijkt dat informatiebeveiliging een belangrijke voorwaarde is voor privacy, terwijl omgekeerd de zorgvuldige omgang met persoonsgegevens noodzakelijk is voor informatiebeveiliging. Informatiebeveiliging en privacy staan naast elkaar en zijn van elkaar afhankelijk, en worden daarom samengevoegd tot één proces: IBP.

Dit beleid, verder te benoemen als IBP-beleid, vormt de basis om informatiebeveiliging en privacy binnen WijWijzer te regelen en vormt de kapstok voor de onderliggende afspraken en procedures.

3. Doel en reikwijdte

3.1. Doel

Informatiebeveiliging en privacy heeft de volgende doelen:

- Het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering.
- Het garanderen van de privacy van alle betrokkenen waarvan WijWijzer persoonsgegevens verwerkt, waaronder leerlingen, hun ouders/verzorgers en medewerkers.
- Beveiligings- en privacy-incidenten voorkomen en de eventuele gevolgen hiervan beperken.

Het informatiebeveiligings- en privacy beleid (IBP-beleid) is erop gericht om de kwaliteit van de verwerking van informatie en de beveiliging van persoonsgegevens te optimaliseren waarbij er een juiste balans moet zijn tussen privacy, functionaliteit en veiligheid. Het uitgangspunt is dat de persoonlijke levenssfeer van de betrokkene (o.a. medewerkers, leerlingen en hun ouders/verzorgers) wordt gerespecteerd en WijWijzer voldoet aan relevante wet- en regelgeving.

3.2. Reikwijdte

- Het IBP-beleid binnen WijWijzer geldt voor alle medewerkers, leerlingen, ouders/verzorgers, (geregistreeerde) bezoekers en externe relaties (inhuur/outsourcing/ZZP). Onder dit beleid vallen ook alle devices van waar geautoriseerde toegang tot het schoolnetwerk verkregen kan worden.
- Het IBP-beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen WijWijzer waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreeerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op overige betrokkenen (zoals stagiairs) waarvan WijWijzer persoonsgegevens verwerkt.
- Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van WijWijzer. Hieronder valt tevens de gecontroleerde informatie, die door de school zelf is gegenereerd en wordt beheerd en de niet-gecontroleerde informatie waarop de school kan worden aangesproken. Voorbeelden hiervan zijn: informatie op onze (school)websites en uitspraken van medewerkers op sociale media.
- Het IBP-beleid geldt voor de geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens, die plaatsvindt onder de verantwoordelijkheid van WijWijzer evenals op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Het IBP-beleid is ook van toepassing op niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.
- IBP-beleid heeft binnen WijWijzer raakvlakken met:
 - Algemeen veiligheids- en toegangsbeveiligingsbeleid; met als aandachtspunten bedrijfshulpverlening, fysieke toegang en beveiliging, crisismanagement, huisvesting en ongevallen.
 - Personeels- en organisatiebeleid; met als aandachtspunten in- en uitstroom van medewerkers, functiewisselingen, functiescheiding en vertrouwensfuncties.
 - ICT-beleid; met als aandachtspunten aanschaf, beheer en gebruik van ict en (digitale) leermiddelen.
 - Medezeggenschap van leerlingenraden, hun ouders/verzorgers en medewerkers.

4. Beleid: hoe doen we dat?

WijWijzer hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

- Het schoolbestuur van WijWijzer neemt de verantwoordelijkheid om ervoor te zorgen dat informatiebeveiliging en privacy geregeld wordt. Het bestuur is hierop aan te spreken en legt hier verantwoording over af. In termen van de wet is het bestuur de verwerkingsverantwoordelijke.
- WijWijzer voldoet aan alle relevante wet- en regelgeving.
- Bij WijWijzer is de verwerking van persoonsgegevens altijd gekoppeld aan een specifiek doel en gebaseerd op één van de wettelijke grondslagen. Een goede balans tussen het belang van WijWijzer om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot het gebruik van zijn/haar persoonsgegevens is essentieel. Bij alle verwerkingen van persoonsgegevens op basis van toestemming kunnen betrokkenen te allen tijde hun toestemming herzien.
- WijWijzer zal alle betrokkenen helder en actief informeren over de verwerkingen van persoonsgegevens, die zowel direct als indirect zijn verkregen. Ook worden alle betrokkenen gewezen op hun rechten met betrekking tot informatie, inzage, verbetering, het wissen van gegevens, beperking van verwerking, verzet, dataportabiliteit en profilering. Dit wordt in het privacyreglement toegelicht.
- WijWijzer legt alle verwerkingen van persoonsgegevens vast in een verwerkingsregister en zal deze up-to-date houden. WijWijzer voldoet hiermee aan de documentatieplicht.
- Binnen WijWijzer is het veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van iedereen. Hierbij hoort niet alleen het actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie, maar ook van papieren documenten.
- WijWijzer is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert de school informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. Medewerkers en leerlingen worden goed geïnformeerd over de regelgeving rondom het gebruik van informatie.
- WijWijzer classificeert informatie en informatiesystemen. De classificatie is het uitgangspunt voor de risicoanalyse en de te nemen maatregelen. Er is een balans tussen de risico's die we willen afdekken en de benodigde investeringen en de te nemen maatregelen.
- WijWijzer sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) verwerkersovereenkomsten af als zij, in opdracht van de school, persoonsgegevens verwerken. Dit geldt ook voor andere organisaties indien er gegevens van leerlingen of medewerkers worden verstrekt.
- WijWijzer verwacht van alle medewerkers, leerlingen, (geregistreerde) bezoekers en externe relaties dat zij zich 'fatsoenlijk' gedragen met een eigen verantwoordelijkheid. Het is niet

acceptabel dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagooverlies. WijWijzer heeft hiervoor gedragscodes geformuleerd, vastgesteld en geïmplementeerd.

- Informatiebeveiliging en privacy is bij WijWijzer een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.
- WijWijzer kijkt bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen vóóraf naar de impact hiervan op de informatiebeveiliging en privacy, zodat tijdig de juiste maatregelen genomen kunnen worden.
- WijWijzer neemt passende technische (beveiligings-)maatregelen om persoonsgegevens en overige data te beschermen tegen de risico's, die de voortgang van het onderwijs, de privacy en de bedrijfsvoering kunnen verstoren. Omdat (een deel van) de infrastructuur elders beheerd wordt, heeft WijWijzer aanvullende afspraken vastgelegd over de technische maatregelen.
- WijWijzer zorgt voor vastlegging van alle beveiligingsincidenten en handelt datalekken volgens een vast protocol af, zo nodig bij melding bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen.

5. Uitwerking van het beleid: wat doen we?

Dit hoofdstuk geeft een praktische invulling van bovenstaande beleidspunten en is daarmee de minimale invulling van het beleid.

5.1. Relevante wet- en regelgeving

De uitwerking van het beleid voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

- Wet op het primair onderwijs en/of Wet voortgezet onderwijs en/of Wet op de expertisecentra
- Wet goed onderwijs en goed bestuur PO/VO
- Wet onderwijstoezicht
- Wet bescherming persoonsgegevens (Wbp; tot 25 mei 2018)
- Algemene Verordening Gegevensbescherming (AVG; vanaf 25 mei 2018)
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht

De internationale norm voor informatiebeveiliging NEN-ISO/IEC 27001 en 27002 (2015) is leidend voor de te nemen beveiligingsmaatregelen.

De bepalingen van de meest recente versie van het convenant 'Digitale onderwijsmiddelen en privacy' zijn leidend bij het maken van afspraken met leveranciers, die in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerken.

5.2. Basisregels bij het omgaan met persoonsgegevens

Bij het verwerken van persoonsgegevens zijn de wettelijke beginselen inzake verwerking persoonsgegevens (art. 5 AVG) leidend. Deze zijn samengevat in de vijf vuistregels met betrekking tot de omgang met persoonsgegevens te weten:

1. **Doelbepaling en doelbinding:** persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld. Persoonsgegevens worden niet verder verwerkt op een manier die onverenigbaar is met de doelen waarvoor ze zijn verkregen.
2. **Grondslag:** verwerking van persoonsgegevens is gebaseerd op een van de zes wettelijke grondslagen.
3. **Dataminimalisatie:** bij de verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt: het type persoonsgegevens moet redelijkerwijs nodig zijn om het doel te bereiken; ze staan in verhouding tot het doel (proportioneel). Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt (subsidiar). Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.
4. **Transparantie:** de school legt aan betrokkenen (leerlingen, hun ouders en medewerkers) op transparante wijze verantwoording af over het gebruik van hun persoonsgegevens, alsmede over het gevoerde IBP-beleid. Deze informatievoorziening vindt ongevraagd plaats. Daarnaast hebben betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun persoonsgegevens. Tevens kunnen betrokkenen zich verzetten tegen het gebruik van hun gegevens.
5. **Data-integriteit:** er zijn maatregelen getroffen om te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn.

5.3. Ondersteunende richtlijnen en procedures

Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen geven invulling aan de uitwerking van het beleid. Bijlage 1 geeft een overzicht van de diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen. Daarnaast worden alle verwerkingen van persoonsgegevens vastgelegd en up-to-date gehouden in een dataregister.

5.4. Voorlichting en bewustzijn

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. De mens is hier een belangrijke factor. Daarom wordt het bewustzijn van de individuele medewerkers voortdurend aangescherpt, zodat de kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het beleid zijn de regelmatig terugkerende bewustwordingscampagnes voor medewerkers, leerlingen en gasten. Verhoging van het IBP-bewustzijn is een gezamenlijke verantwoordelijkheid van de verantwoordelijke IBP, de FG, en de Security Officer met het bestuur als eindverantwoordelijke.

5.5. Classificatie en risicoanalyse

Alle informatie heeft waarde, daarom worden alle gegevens en informatiesystemen waarop dit beleid van toepassing is, geclassificeerd. Het niveau van de te nemen beveiligingsmaatregelen is afhankelijk van de classificatie. De classificatie van informatie is afhankelijk van de gegevens in het

informatiesysteem en wordt bepaald op basis van risicoanalyses. Daarbij zijn beschikbaarheid, integriteit en vertrouwelijkheid de betrouwbaarheidsaspecten die van belang zijn.

Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, wordt vóóraf gekeken naar de impact van de ontwikkelingen en de beoogde verwerkingen op informatiebeveiliging en privacy, zodat passende maatregelen genomen kunnen worden. Vanaf de start van nieuwe (ict)projecten wordt rekening gehouden met informatiebeveiliging en privacy.

5.6. Incidenten en datalekken

Alle medewerkers, die een beveiligingsincident of datalek vermoeden, dienen dit te melden. Het melden van beveiligingsincidenten en datalekken is vastgelegd in een protocol. De afhandeling van deze incidenten volgt conform een gestructureerd proces, dat ook voorziet in de juiste stappen rondom de meldplicht datalekken. Alle (beveiligings)incidenten worden vastgelegd in een incidentenregister.

Alle (beveiligings)incidenten kunnen worden gemeld bij **datalek@wijwijzer.nu** of via het formulier op intranet.

Periodiek zullen de beveiligingsincidenten besproken worden en waar nodig aanvullende passende beleidsmaatregelen genomen worden.

5.7. Planning en controle

Dit IBP-beleid wordt minimaal elke vier jaar getoetst en bijgesteld door het bestuur. Hierbij wordt rekening gehouden met:

- De status van de informatiebeveiliging als geheel (beleid, organisatie, risico's);
- De actuele geïnventariseerde risico's;
- De effectiviteit van de genomen maatregelen en aantoonbare werking daarvan

Daarnaast kent WijWijzer een jaarlijkse planning en control cyclus voor informatiebeveiliging en privacy. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het informatiebeveiligings- en privacybeleid wordt getoetst. Tevens worden hier actuele ontwikkelingen op het gebied van techniek, wet- en regelgeving etc meegenomen.

Wanneer er zich omstandigheden voordoen waaruit blijkt dat het IBP-beleid of andere ondersteunende richtlijnen en procedures aangepast moeten worden, past het bestuur de inhoud hiervan aan in overleg met de direct betrokkenen (b.v. directeuren en staf) en communiceert hier actief over, zodat alle betrokkenen op de hoogte zijn.

5.8. Naleving en sancties

De naleving bestaat uit algemeen toezicht in de dagelijkse praktijk op de naleving van beleid en richtlijnen. Van belang hierbij is dat leidinggevend en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Er wordt actief aandacht besteed aan IBP bij de aanstelling van nieuwe medewerkers, tijdens functioneringsgesprekken, met een bovenschoolse gedragscode, met periodieke bewustwordingscampagnes, etc.

Voor toezicht op de naleving van de AVG vervult de Functionaris voor Gegevensbescherming (FG) een belangrijke rol. De FG wordt aangesteld door het bestuur, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt via een door het bestuur vast te stellen

Regeling taken en verantwoordelijkheden Functionaris voor Gegevensbescherming. De FG is bij WijWijzer extern belegd via Privacy op School.

Mocht de naleving van dit beleid ernstig tekortschieten, dan kan WijWijzer de betrokken verantwoordelijke medewerkers een sanctie opleggen binnen de kaders van de CAO en de wettelijke mogelijkheden. Op welke manier WijWijzer dit doet, staat beschreven in de Gedragscodes voor medewerkers.

5.9. Logging en monitoring

Logging en monitoring door de ICT-afdeling zorgt ervoor dat gebeurtenissen met betrekking tot geautomatiseerde systemen en toegang tot gegevens worden vastgelegd. Hieronder vallen onder andere het in- en uitloggen van gebruikers en (poging) tot ongeautoriseerde toegang tot het netwerk.

6. Organisatie: wie doet wat?

6.1. Rollen en verantwoordelijkheden

De organisatie van IBP gaat over processen, gewoontes, beleid, wetten en regels die van betekenis zijn voor de manier waarop mensen een organisatie sturen, besturen, beheren en controleren. Hierbij spelen de relaties tussen de verschillende betrokkenen en de doelen van de organisatie een rol.

6.2. Richtinggevend

Eindverantwoordelijke

Het College van Bestuur is eindverantwoordelijk voor IBP en stelt het beleid en de basismaatregelen op het gebied van informatiebeveiliging en privacy vast. De toepassing en werking van het IBP-beleid wordt op basis van regelmatige rapportages geëvalueerd. De inhoudelijke verantwoordelijkheid voor IBP is gemandateerd aan de bestuurssecretaris en de beleidsmedewerker Onderwijs en Innovatie (het AVG team).

6.3. Sturend

Bestuurssecretaris (Privacy Officer)

De bestuurssecretaris is een rol op sturend niveau (Privacy Officer). Hij/zij geeft samen met de beleidsmedewerker Onderwijs en Innovatie terugkoppeling en advies aan de eindverantwoordelijke (het bestuur) en stuurt de mensen aan op uitvoerend niveau.

De bestuurssecretaris en de beleidsmedewerker Onderwijs en Innovatie moeten:

- Het beleid vertalen naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling,
- De uniformiteit bewaken binnen WijWijzer,
- Het aanspreekpunt zijn voor incidenten op het gebied van informatiebeveiliging en privacy,
- De verdere afhandeling van incidenten binnen WijWijzer coördineren

Functionaris voor Gegevensbescherming

De functionaris voor gegevensbescherming (FG), houdt binnen WijWijzer op afstand toezicht op de toepassing en naleving van de AVG. De wettelijke taken en bevoegdheden van de FG geven deze

functionaris een onafhankelijke positie in de organisatie. De FG zorgt voor het verbeteren en stimuleren van bewustwording rondom IBP, het afhandelen van informatiebeveiligingsincidenten, adviseert over het regelen van privacy, onderhoudt zo nodig de contacten met de Autoriteit Persoonsgegevens (AP) en rapporteert aan de eindverantwoordelijke (het bestuur). De FG heeft regelmatig overleg met de bestuurssecretaris en de beleidsmedewerker Onderwijs en Innovatie. De FG is ook de contactpersoon voor klachten en vragen van betrokkenen.

6.4. Domeinverantwoordelijke

Binnen de stichting zijn er verschillende domeinen, zoals ICT, personeel, administratie, facilitaire zaken, huisvesting, financiën, onderwijskwaliteit etc. Op elk van deze domeinen is iemand verantwoordelijk om te bepalen op welke wijze IBP daarbinnen wordt vormgegeven in richtlijnen, procedures en instructies in overleg met de bestuurssecretaris en de beleidsmedewerker Onderwijs en Innovatie.

Deze domeinverantwoordelijke is tevens verantwoordelijk voor de risico's die veroorzaakt worden doordat personen of applicaties ten onrechte toegang krijgen tot applicaties. Om deze risico's te verkleinen hebben proceseigenaren de volgende specifieke taken:

- Samen met de eindverantwoordelijke stellen zij het beleid voor toegang (autorisaties) vast: periodiek actualiseren de domeinverantwoordelijken een overzicht van applicaties waarbij gegevens worden verwerkt.
- Samen met functioneel beheer en ICT-beheer zien zij er op toe dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn en voor hun werkzaamheden toegang toe moeten hebben.
- Samen met functioneel beheer en ICT-beheer beoordelen zij periodiek de toegangsrechten van de gebruikers.

6.4. Uitvoerend

Security Officer (SO)

De Security Officer vormt een technisch aanspreekpunt als het gaat over informatiebeveiliging voor de directie en de medewerkers. Bij WijWijzer is dit belegd bij de beleidsmedewerker Onderwijs en Innovatie

Functioneel beheerder of applicatiebeheerder

Ieder softwarepakket of (web-)applicatie heeft een beheerder. Bij vragen over de software of applicatie is bekend wie daarvoor aangesproken kan worden. De functioneel beheerder wordt vanuit de domeinverantwoordelijke voorzien van een ingevuld werkpakket, bestaande uit richtlijnen, procedures en instructies. Op basis hiervan voert hij zijn of haar taken uit.

In samenwerking met de ICT-ers wordt een 'digitaal landschap' opgesteld waarin overzicht van bovenstaande wordt gegeven.

Medewerkers

Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging en privacy in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in o.a. het Handboek privacy en informatiebeleid en de Gedragscode verantwoord gebruik van bedrijfsmiddelen. Daarnaast worden medewerkers in hun dagelijkse werkzaamheden, waar nodig, ondersteund met checklists en formulieren.

Medewerkers worden gevraagd om actief betrokken te zijn bij informatiebeveiliging. Dit kan door meldingen te maken van beveiligingsincidenten of datalekken, het doen van verbetervoorstellen en

het uitoefenen van invloed op het beleid (individueel, in groepsverband zoals het ICT-netwerk of via de (G)MR).

Leidinggevende/schooldirecteur

Naleving van het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende heeft op uitvoerend niveau de taak om:

- Er voor te zorgen dat zijn medewerkers op de hoogte zijn van het IBP-beleid;
- Toe te zien op de naleving van het IBP-beleid door de medewerkers, waarbij hij/zij zelf een voorbeeldfunctie heeft;
- Periodiek het onderwerp IBP onder de aandacht te brengen in werkoverleggen, beoordelingen etc.;
- Als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde IBP-onderwerpen.

De leidinggevende kan in zijn taak ondersteund worden door het AVG-team. Leidinggevend en hebben hierbij een voorbeeldrol ten opzichte van hun medewerkers.

IBP-team

Een IBP-team (bestuurssecretaris en beleidsmedewerker onderwijs en innovatie) wordt organisatiebreed zowel preventief als curatief benoemd voor informatiebeveiliging en privacy-incidenten. De leden van het IBP-team zijn benoemd door de eindverantwoordelijke en handelen in diens opdracht.

Het IBP-team van WijWijzer heeft de volgende opdracht:

- Het signaleren en registreren van alle privacy verzoeken, beveiligingsincidenten en datalekken. Het coördineren van de maatregelen en het toezien op de oplossing van problemen die tot incidenten hebben geleid of waardoor de incidenten zijn veroorzaakt (of het bieden van ondersteuning daarbij);
- Het geven van voorlichting en het doen van algemene aanbevelingen aan netwerkbeheerders, systeembeheerders, ontwikkelaars en eindgebruikers door het verspreiden van informatie;
- Het leveren van managementrapportages en verbetervoorstellen aan de domeinverantwoordelijke over de beveiligingsincidenten (Privacy Officer) en verzoeken tot uitoefening van de privacyrechten van de betrokkenen.

Bij een calamiteit kan het IBP-team terstond bij elkaar worden geroepen, in opdracht van het bestuur. Het doel hiervan is om de continuïteit van de informatievoorziening en de privacy te waarborgen. Onder calamiteiten worden verstaan:

- Datalek;
- Grote verstoringen van het netwerk (bijvoorbeeld DDoS aanval);
- Natuurrampen (brand, overstroming, storm, etc.).

Het IBP-team bij WijWijzer behandelt meldingen vertrouwelijk en verstrekt alleen informatie over beveiliging en privacy-incidenten als dat noodzakelijk en relevant is voor de oplossing van een incident.

BIJLAGE 1: Ondersteunende regelingen en procedures

Deze bijlage bevat een aantal aanvullende beleidsstukken, regelingen, procedures en protocollen. Een aantal is vanuit de Algemene Verordening Gegevensbescherming verplicht.

Verplicht vanuit de AVG:

- Regeling taken en verantwoordelijkheden Functionaris voor Gegevensbescherming (FG)
- Procedure melden beveiligingsincidenten en datalekken
- Procedure organiseren van verwerkersovereenkomsten
- Procedure gegevensbeschermingseffectbeoordeling (DPIA, risicoanalyse)

Overige documenten:

- Handboek privacy en informatiebeleid (voor medewerkers)
- Privacyreglement
- Wachtwoordbeleid
- Geheimhoudings- en privacyverklaring externen (ook: stagiaires, vrijwilligers)
- Gedragscode voor leerlingen verantwoord gebruik van ICT en internet (responsible disclosure)
- Gedragscode voor medewerkers verantwoord gebruik van ICT en internet (responsible disclosure)
- Procedure voor verwijderen van gegevens (bewaartermijnen)
- Procesbeschrijving rechten betrokkenen (autorisatiematrix)
- Procedure toestemming gebruik beeldmateriaal (incl. toestemmingsbrief eenmalig)
- Reglement Cameratoezicht
- Procedure rondom uitwisselen gegevens (passend onderwijs, leerling dossiers, leerplicht enz), waaronder kinderopvang

BIJLAGE 2: Overzicht van rollen en verantwoordelijkheden en taken

Onderstaand overzicht geeft aan welke verantwoordelijkheden en taken bij welke rollen horen bij WijWijzer.

Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen
Richting-gevend (strategisch)	Voorbeelden: Bestuur CvB Directeur	• Eindverantwoordelijk • IBP-beleidsvorming, -vastlegging en het uitdragen ervan • Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens • Evalueren toepassing en werking IBP-beleid op basis van rapportages • Organisatie IBP inrichten	• Informatiebeveiligings- en privacy beleid • Baseline / basismaatregelen • Reglement FG vaststellen • Privacyreglement vaststellen
	Privacy Officer (de persoon die inhoudelijk verantwoordelijk is voor IBP) i.s.m. Security Officer	• Inhoudelijk verantwoordelijk voor IBP • IBP-planning en controle • Adviseert bestuur/CvB/directie over IBP • Voorbereiden uitvoeren IBP-beleid, classificatie/risicoanalyse • Hanteren IBP normen en wijze van toetsen • Evalueren IBP-beleid en maatregelen • Uitwerken algemeen beleid naar specifiek beleid op een uniforme wijze • Schrijven en beheren van processen, richtlijnen en procedures om de uitvoering te ondersteunen	Processen, richtlijnen en procedures IBP, waaronder: • Activiteitenkalender • Protocol beveiligingsincidenten en datalekken • Verwerkersovereenkomsten regelen • Brief toestemming gebruik beeldmateriaal • Opstellen informatie documentatie richting leerlingen, ouders / verzorgers • Security awareness activiteiten • Sociale media reglement • Gedragscode ict en internetgebruik • Gedragscode medewerkers en leerlingen
	Functionaris voor Gegevens-bescherming en/of Privacy officer	• Toezicht op naleving privacy wetgeving • Voorlichting privacy en stimuleren bewustwording • Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens • Afwikkeling klachten en incidenten	• Privacyreglement, • procedure IBP-incident afhandeling • Inrichten meldpunt datalekken

	Domeinverantwoordelijke/ Proceseigenaren Waaronder o.a.: ICT, P&O, facilitair, onderwijs, financiën, administratie	• Classificatie / risicoanalyse in samenwerking met privacy officer en security officer • Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door bestuur/CvB/directie • Samen met functioneel beheer en ICT beheer er op toezien dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn. • Samen met functioneel beheer en ICT beheer de toegangsrechten van gebruikers regelmatig beoordelen en controleren.	• Inventariseren waar persoonsgegevens van de school terechtkomen (leveranciers lijst); input vewerkingsregister • Classificatie- en risicoanalyse documenten. Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder: • Toegangsmatrix diverse informatiesystemen en netwerk
--	--	---	--

Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen
Richting-gevend (strategisch)	Voorbeelden: Bestuur CvB Directeur	• Eindverantwoordelijk • IBP-beleidsvorming, -vastlegging en het uitdragen ervan • Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens • Evalueren toepassing en werking IBP-beleid op basis van rapportages • Organisatie IBP inrichten	• Informatiebeveiligings- en privacy beleid • Baseline / basismaatregelen • Reglement FG vaststellen • Privacyreglement vaststellen
	Manager IBP, Verantwoordelijke IBP, informatiemanager of privacy officer (de persoon die inhoudelijk)	• Inhoudelijk verantwoordelijk voor IBP • IBP-planning en controle • Adviseert bestuur/CvB/directie over IBP • Voorbereiden uitvoeren IBP-beleid, Classificatie/risicoanalyse • Hanteren IBP normen en wijze van toetsen • Evalueren IBP-beleid en maatregelen • Uitwerken algemeen beleid naar specifiek beleid op een uniforme wijze	Processen, richtlijnen en procedures IBP, waaronder: • Activiteitenkalender • Protocol beveiligingsincidenten en datalekken • Verwerkersovereenkomsten regelen • Brief toestemming gebruik beeldmateriaal • Opstellen informatie documentatie richting leerlingen, ouders / verzorgers • Security awareness activiteiten

	verantwoordelijk is voor IBP)	• Schrijven en beheren van processen, richtlijnen en procedures om de uitvoering te ondersteunen	• Sociale media reglement • Gedragscode ict en internetgebruik • Gedragscode medewerkers en leerlingen
	Functionaris voor Gegevensbescherming en/of Privacy officer	• Toezicht op naleving privacy wetgeving • Voorlichting privacy en stimuleren bewustwording • Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens • Afwikkeling klachten en incidenten	• Privacyreglement, • procedure IBP-incident afhandeling • Inrichten meldpunt datalekken
	Domeinverantwoordelijke/ Proceseigenaren Waaronder o.a.: ICT, HRM / P&O, facilitair, onderwijs, financiën, inkoop en administratie	• Classificatie / risicoanalyse in samenwerking met Manager IBP (Informatiemanager / verantwoordelijke IBP / privacy officer) • Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door bestuur/CvB/directie • Samen met functioneel beheer en ICT beheer er op toezien dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn. • Samen met functioneel beheer en ICT beheer de toegangsrechten van gebruikers regelmatig beoordelen en controleren.	• Inventariseren waar persoonsgegevens van de school terechtkomen (leveranciers lijst); input dataregister • Classificatie- en risicoanalyse documenten. Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder: • Toegangsmatrix diverse informatiesystemen en netwerk

Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen
Uitvoerend (operationeel)	Security officer Privacy officer / communicatie adviseur Dagelijkse leiding / leidinggevende / directie Medewerkers	• Incidentafhandeling (registreren en evalueren). • Technisch aanspreekpunt voor IBP-incidenten. • Uitvoeren taken conform gegeven richtlijnen en procedures. • Communicatie naar alle betrokkenen; er voor zorgen dat medewerkers op de hoogte zijn van het IBP-beleid en de consequenties ervan. • Toezien op de naleving van het IBP-beleid en de daarbij behorende processen, richtlijnen en procedures door de medewerkers. • Voorbeeldfunctie met positieve en actieve houding t.a.v. IBP-beleid. • Implementeren IBP-maatregelen. • periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen, beoordelingen etc.; • Rapporteren voortgang m.b.t. doelstellingen IBP-beleid aan bestuur. • Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden.	Communiceren, informeren en toezien op naleving van o.a.: • IBP in het algemeen • Regels passend onderwijs • Hoe omgaan met leerling dossiers • Wie mogen wat zien • Gedragscode • Omgaan met sociale media • Mediawijs maken